15. (Amended) A system as claimed in Claim 11, [further comprising a server for accessing the storage means,] characterized in that

the server is further configured:

[for reading] to read from the storage means [an encrypted private key and] a corresponding public key associated with [an] the ID [corresponding to a particular user, for transmitting the encrypted private key to the particular user,] and

[for decrypting] to decrypt data received from the particular user using the ~~public key~~.

16. (Amended) A system as claimed in Claim 12, [further comprising a server for accessing the storage means,] characterized in that

the server is further configured:

[for reading] to read from the storage means [an encrypted private key and] a corresponding public key associated with [an] the ID [corresponding to a particular user, for transmitting the encrypted private key to the particular user,] and

[for decrypting] to decrypt data received from the particular user using the public key.

REMARKS

The Examiner has objected to claim 11, and has provided specific suggestions. The Applicant respectfully requests the Examiner's reconsideration of this objection in view of the above amendment to claim 11.

The Examiner has rejected claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over Dolan (US 5,604,801) in view of Krajewski (US 5,590,199). The Applicant respectfully traverses this rejection. Claim 11 is amended herein to particularly point out and distinctly claim the subject matter that the Applicant views as the invention, in view of Dolan.

The Applicant specifically teaches and claims a system and methods wherein a server stores a user's private key in encrypted form, and communicates the encrypted private key to the user as required. By providing the encrypted private key from the

server to the user, the user is free to encrypt, decrypt, or sign documents via any terminal device, or client processor, that is networked to the server. The user communicates a user ID to the server, and in response, the server communicates the encrypted private key. The user decrypts the encrypted private key, using whatever parameters were used to encrypt the private key, such as the user's fingerprints, a password, a pass-phrase, and so on. After decrypting the private key, the user can use the private key to effect cryptographic operations, such as encryption, decryption and signing, or authentication. In this manner, the user is not required to retain a copy of private key, via, for example, a smart-card or other memory device.

Dolan also teaches the storage of a user's private key in an encrypted form at the server. In Dolan, however, the user communicates an encrypted key-decrypting key to the server (block 481 of FIG. 4a of Dolan). The server decrypts the key-decrypting key (block 492 of FIG. 4b of Dolan), then decrypts the user's private key using the decrypted key-decrypting key (block 493 of FIG. 4b of Dolan), and then encrypts a message from the user using the user's private key (block 494 of FIG. 4b of Dolan). That is, the encrypted user's private key remains at the server at all times, and, because of this, only the server is able to perform cryptographic functions using the user's private key. In Dolan, a message that is intended to be encrypted or signed by the server must be transmitted in an insecure form to the server (block 482).

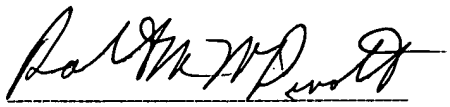
As the Examiner notes, Dolan does not disclose communicating the encrypted private key, and asserts that Krajewski discloses receiving the encrypted private key at the user's location and decrypting the received encrypted private key. The Applicant respectfully suggests that the Examiner has mis-characterized Krajewski.

Krajewski teaches a dual-storage of the user's private key. The user's private key is stored in the user's smart-card 30 in an encrypted form, and at the server site KAS 32 in an unencrypted form (Krajewski column 5, lines 1-8; and again at lines 60-63). Krajewski's server 32 uses the user's private key to encrypt a session key that is associated with a ticket, and subsequently communicates the ticket and session key to the user. The user then decrypts the session key using the user's private key that is contained in the smart-card 30 (Krajewski column 6, lines 21-24). Krajewski neither teaches nor suggests communicating the private key to the user, because, according to Krajewski, the

user's private key is stored in the user's smart-card (Krajewski column 5, lines 55-63). As noted by the Applicant in the background of the invention, the use of a smart-card requires that each terminal device or client processor must contain a smart-card reading device (Applicant's page 2, lines 19-22). As also noted by the Applicant, the storage of user private keys in an unsecured form on a common server can lead to catastrophic failures of the intended security system, when, for example, an intruder gains access to the server that contains the unsecured private key of each user in a network (Applicant's page 3, lines 12-16). Krajewski neither teaches nor suggests communicating an encrypted private key from the server to the location of the user, as specifically claimed by the Applicant in each independent claim (claims 1, 5, and 11, as amended).

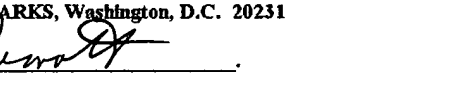
Because neither Dolan nor Krajewski, individually or collectively, teach or suggest the communication of encrypted private keys to users upon receipt of a user ID, as specifically taught and claimed by the Applicant, the Applicant respectfully requests the Examiner's reconsideration of the rejection of claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over Dolan in view of Krajewski, and respectfully requests the subsequent allowance of all claims.

Respectfully submitted,



Robert M. McDermott, Esq.
Reg. No. 41,508
203-544-8889

**CERTIFICATE OF MAILING**
**It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231**

**On** 5 January 2000 **By**  .